I. Purpose

Lansing Community College regards its information assets as one of its most important assets. Information Security provides protections to ensure the security, integrity and confidentiality of LCC's information assets by identifying the risks of accidental and intentional disclosure of, or damage to, the information and implementing protective measures to manage those risks.

II. Scope

This policy covers all information assets, including computers and communication devices used, maintained, owned and/or operated by Lansing Community College as well as LCC owned information stored on a remote system operated by an outside entity. This policy also covers any computer or communications device that is present on Lansing Community College premises and/or use Lansing Community College communication infrastructure, but which may not be owned or operated by Lansing Community College.

Information that is in the custody of Lansing Community College and entrusted to an entity outside of Lansing Community College by means of a contracted service or partnership must be afforded the same protection as similar LCC owned information. LCC management will provide the outside entity with a copy of this Information Security Policy and the applicable written standards that specify the level of protection that the outside entity is expected to provide. The outside entity must sign-off on those policies as an indication of understanding and acceptance.

III. Policy/Procedure

A. Authority

The Board of Trustees on the recommendation of the President authorizes the “Information Security Policy”.

B. Organization

Information Security Organization

The Information Security Management System will be modeled after the ISO 27001:2005 standard and will use its process approach to understanding the College’s security requirements and to enact the needed monitoring and

controls. A security strategy of Defense in Depth will be employed to manage the risk to information as required by the classification of the information. The ISO 17799:2005 standard will be used as the basis for evaluating the controls for security of the College's information resources. In addition, Lansing Community College will protect its information assets in a legal and ethical manner and in accordance with good business practice.

Director of Information Security

This position reports to the Executive Director of Administrative Services and is responsible for ensuring that:

1. The Lansing Community College Information Security Policy and Standards are reviewed, maintained, and distributed.
2. Appropriate levels of employee awareness and education on information security are being maintained.
3. Appropriate security measures are being implemented by staff and operating management throughout Lansing Community College.
4. Information Security reviews are conducted throughout Lansing Community College and those staff and operating managers correct deviations from Lansing Community College Information Security Policy and Standards in their respective areas of responsibility.

C. Acceptable Usage

The acceptable and unacceptable uses of LCC information assets are defined within the College's Acceptable Use Policy located on the College Web Site. Lansing Community College provides access to computer and communication resources to facilitate activities that further the mission of the College. A user is expected to only access applications and information that the user has been authorized to access.

D. Categories of responsibility for Information Security Managers

Administrators, faculty leads, or other employees that supervise others as part of their job duties are responsible for all aspects of the use and protection of Lansing Community College information assets within their areas of functional responsibility.

Owners – All information assets must have an identifiable owner, either a manager or a non-manager representing management, who is responsible for identifying, classifying, authorizing access to and protecting specific information assets.

Users – Students, faculty, staff, and consultants who possess a Technology User-id (TUID) are responsible for using appropriate security to safe guard information that they are authorized to access.

Suppliers – Service suppliers of hosting, telecommunications, data storage or operations services have the responsibility for safekeeping and operating functions, in accordance with security measures appropriate for the information assets over which they have custody.

E. Classification of Information Assets

Information assets will be identified by the Information owners to classify the asset's value to the College. The Information Owner will identify the Information assets and will classify the information sensitivity as either public, private or confidential (see the LCC Information Sensitivity Policy for additional policies regarding sensitivity classification). The Information assets will also be classified based on availability, i.e., normal, essential, or critical. These classifications will be used by the College to determine the level of risk associated with the operation of each information resource.

Sensitivity classifications:

Public – Information that is in the public domain or information intended to be communicated to the general public or community. This classification includes course descriptions or information about services of the College.

Private - Information that should not be available to a general population. This classification includes employee procedure manuals, department financial records, salaries and date of birth.

Confidential – This information needs to be safeguarded because of regulation or determination of the College that the loss of this information would cause devastating financial loss or loss of reputation. This classification includes most information about students and employees academic, financial or medical records.

Availability classifications:

Normal – Information assets that have a limited impact to the operations of the College as a whole or information that can be unavailable for up to a week or more.

Essential – Information assets that are used to support operations of the College, but alternate resources can be used or a limited outage of a day or two is acceptable.

Critical – Information assets that are required for operation of the College divisional processes, both academic and administrative (example: telephones, data network).

F. Risk Assessment and Risk Management

Risk Assessment of information assets is a formal process that will describe the risk of the occurrence of threats to LCC and the method chosen to mitigate the threat. This process will result in the creation of a document for review by management that describes the risks, the safeguards that will be employed and the remediation determined to best mitigate any threat or incident involving LCC information assets (see the LCC Risk Assessment Policy and Procedure for additional requirements). An Information Risk Assessment must be performed by each department at least once a year. The management of LCC can choose to:

Accept the risk – This alternative is taken if the probability of occurrence is very low or the cost of protective measures is too great. This alternative could also be used for low value or easily replaceable information, such as expendable supplies or public domain information.

Transfer the risk – This alternative is implemented through use of contractual obligations, such as insurance.

Reduce the risk – This alternative is taken by installing protective measures or by establishing continuity plans.

Owners of Information are responsible for managing the risks to which such information assets are exposed. Owners must determine the criticality of their information assets and classify them according to the need for their availability and their sensitivity. Owners are also responsible for assuring that users and suppliers of services protect information assets at the level specified by implementing a risk management plan.

Input to the risk management process will be acquired from all levels of the organization, with the lower levels of the organization reporting to the higher levels the risks that would impact their operation.

G. Reviewing and Testing

Lansing Community College will periodically (at least annually) assess if current practices provide the desired protections to achieve the intended security objectives. All departments with owners, users or suppliers of services of Lansing Community College information assets must conduct reviews each year to assure compliance with Lansing Community College Information Security Policy and Standards. Independent reviews performed by personnel assigned to the Information Security function must be conducted. The ISO 17799:2005 "Code of practice for information security management" will provide the control framework that the College will test its systems against.

H. Destruction and Declassification of Media

The LCC Information Security Policy requires destruction or declassification of information resources, including waste materials, which were used for recording confidential information when such information is no longer needed. Media that cannot be used again (e.g. paper) must be destroyed and media that can be used again (e.g. magnetic disks) must be either declassified or destroyed beyond recognition and reconstruction. Media declassification means that the critical information recorded on the media is destroyed usually by overwriting or degaussing. The quantity of critical information should be reduced to the minimum necessary.

I. Incident Response

The Lansing Community College Information Security Policy requires the reporting of:

A. Incident of suspected or actual loss or compromise of LCC information, resource or service.
B. Any violation or suspected violation of LCC Information Security Policy or Standards.
C. Any violation or suspected violation of departmental Information Security standards, procedures or guidelines.

The requirements for incident reporting apply to all employees, students, contractors and suppliers of LCC at all times. Such incidents must be reported whether they are intentional or unintentional to abuse@lcc.edu. See the LCC Incident and Response Plan for further requirements regarding incident reporting and response.

J. Education and Awareness

It is the responsibility of individual management, with the assistance of Information Security department, to ensure that all employees who use LCC information resources are adequately trained in security procedures and policy. It is the responsibility of the Student and Academic Support division, with the assistance of the Information Security department, to ensure that all students who use LCC information resources are adequately trained in security procedures and policy.

IV. Responsibility

The Direction of Information Security is responsible for preparing procedures to implement this policy.

V. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and possible civil and/or criminal prosecution to the full extent of the law.

VI. Definitions

Information assets can be in many forms including but not limited to verbal, written, or electronic. Information includes data stored on magnetic or other electronic media, data stored in computer memory, data displayed on a monitor, projector system or other output, data being transmitted over communication lines or verbal, written or printed documents.

Information Security is the protection of information assets regardless of method of storage, presentation or transmission from intentional or accidental disclosure, modification or loss of access.

Controls are hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing it.

Procedure is a set ordered series of steps developed to accomplish a desired result.

Standards are minimal requirements that exist for a particular protective control.

Threats are any activity that represents possible danger to your information. Danger can be thought of as anything that would negatively affect the confidentiality, integrity or availability of your systems or services. (1-9, SANS Security Essentials)

Risk is the likelihood that a particular threat will take advantage of a particular vulnerability.

VII. Revision History

Revised 5/21/2007

Failure to follow this policy may result in disciplinary action up to and including termination.